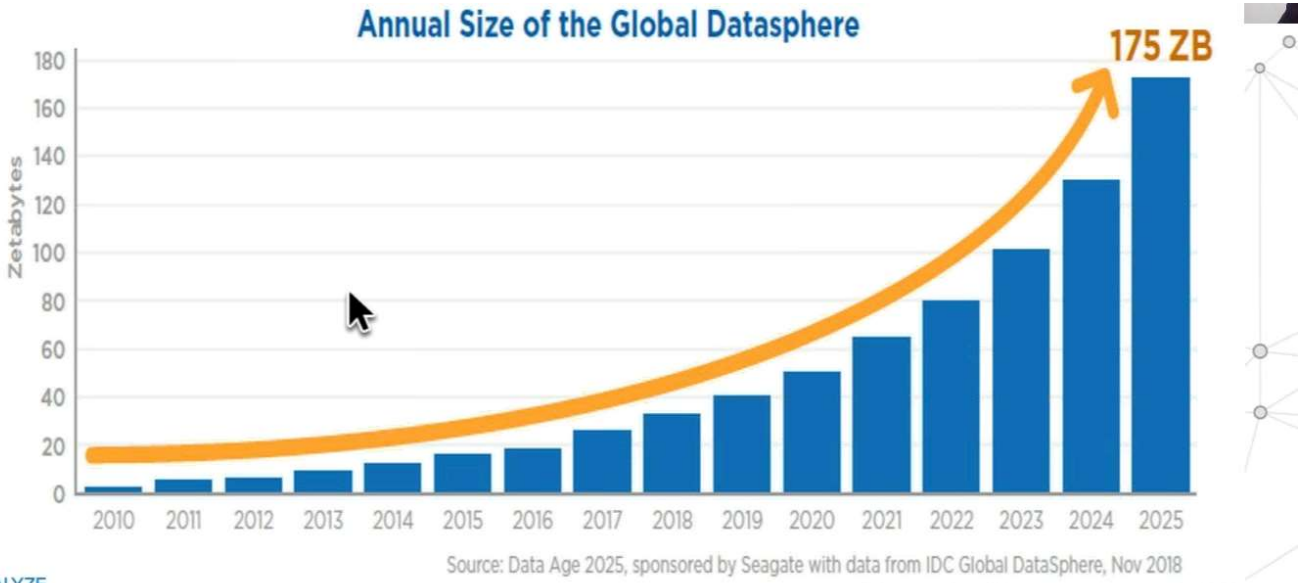
Security Management and Governance: Policies, Procedures, Standards, Baselines, and Guidelines

Dr. Bhaskar Mondal


verizon
Cut to the chase.
Keep your team informed of danger or help stakeholders throughout your organization understand the need for improved security. Get the executive-level view of the latest threats.
Home / Resources /
Read the summary
70%
of breaches were caused by outsiders.
86%
of breaches were financially motivated.
43%
of breaches were attacks on web applications, more than double the results from last year.
27%
of malware incidents can be attributed to ransomware.
2020 Data Breach Investigations Report

Data Growth



IDC ANALYZE THE FUTURE

175 ZB= 175000000000 TB

"IDC predicts that the Global Datasphere will grow from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025."

Challenge

- Organizations are struggling to manage uncontrolled data growth
- Segregation of business-critical data from noncritical data is big challenge

Information Security Pain Points

- What data is critical for the enterprise?
- Where is it residing in the IT ecosystem?
- Who have access to it?
- Which regulation/ compliance I am violating
- Is my company's data secure
- What is my current risk level?

On Information Security

- “If you don’t know what you have, where is it, and why you have it, you can’t expect to apply the appropriate policies and controls to protect it.” – Forrester
- “Focus on controls that broadly address the problem, such as implementing people-centric security data classification. These controls are the foundation upon which additional controls con be built” -- Gartner

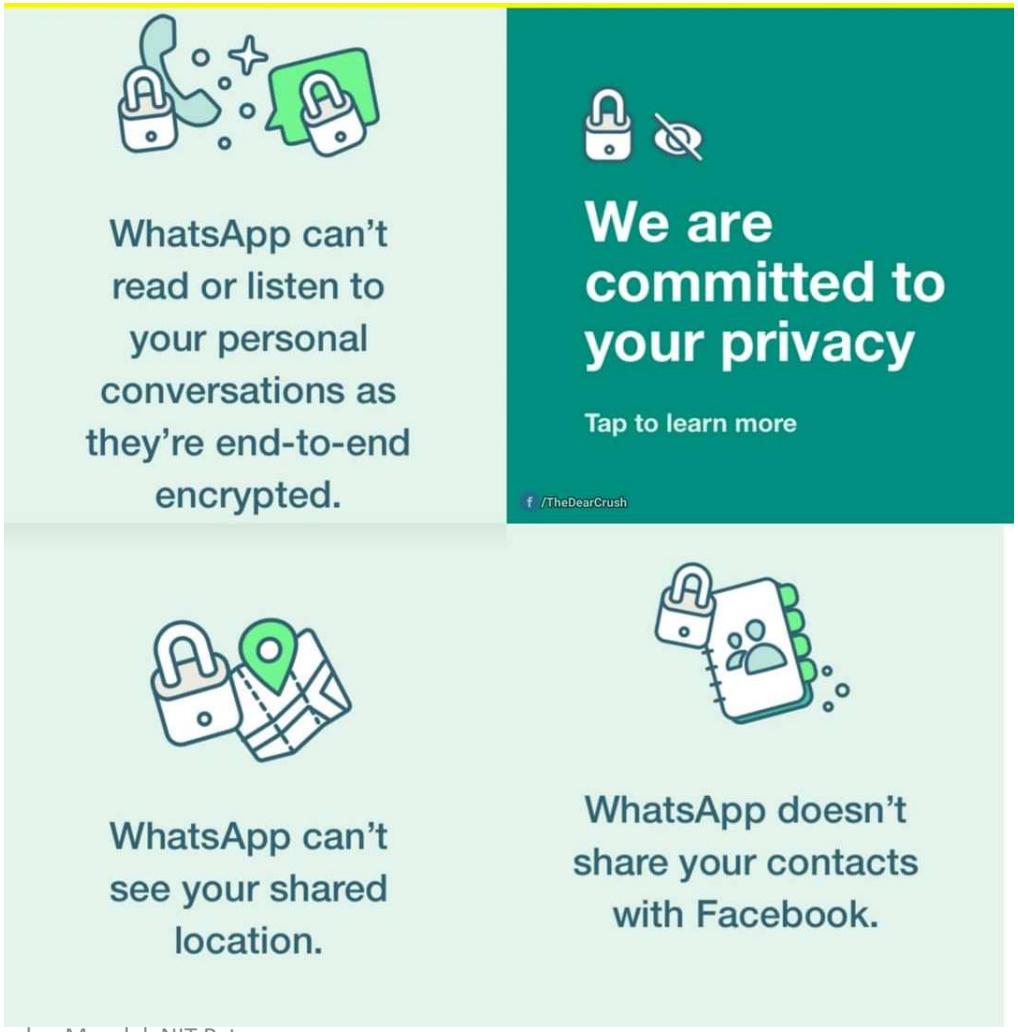
The Hacker's Talk
1 d •

In a massive development in the ongoing TRP scam case, a 500-page document of conversations between Republic TV's Arnab Goswami and Former Chief Executive Officer of Broadcast Audience Research Council (BARC) Partho Das Gupta was allegedly leaked on social media.
The detailed chats reveal damning information related to Goswami's proximity with the Prime Minister's office and members of the ruling government, his efforts to manipulate TRPs in his favour and seek help from the BJP government and much more. Some chats

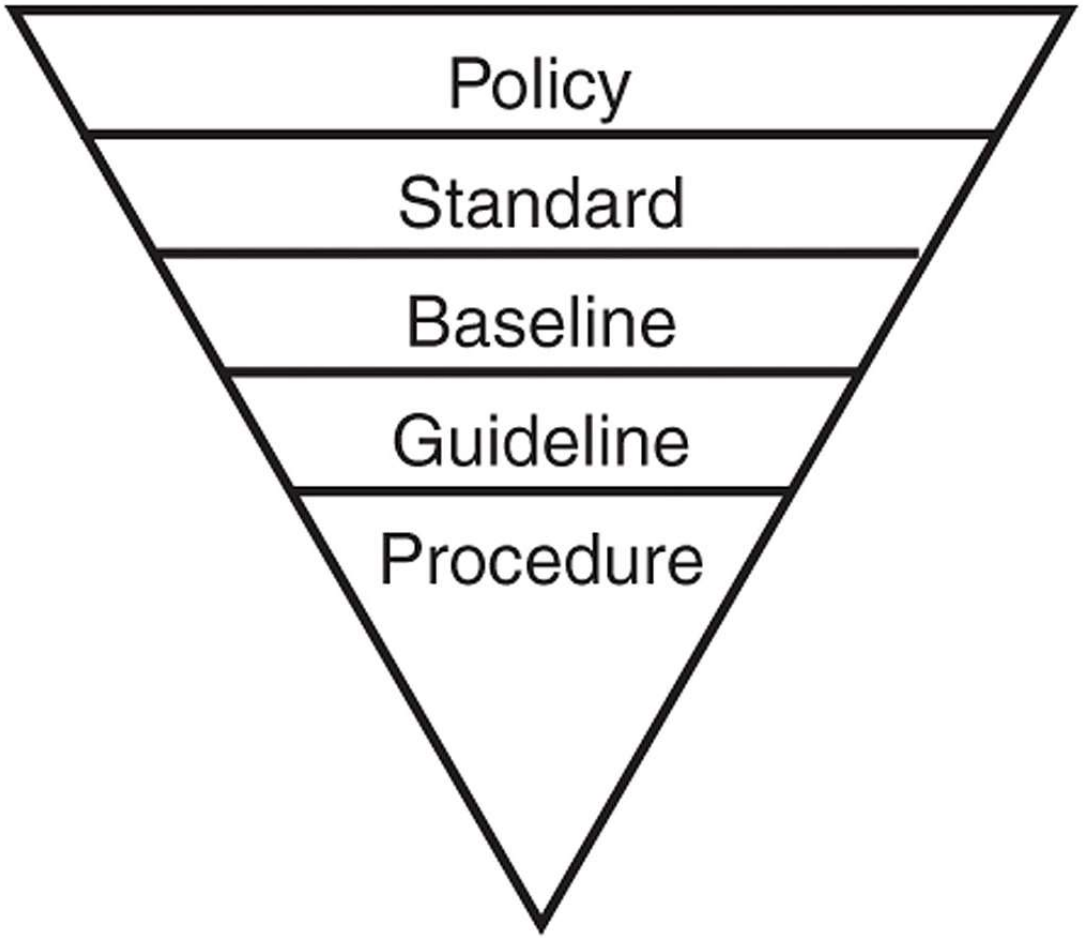
In one of the chat messages circulating online, former BARC CEO allegedly sent a confidential BARC letter to Goswami saying that he had jammed the News Broadcasters Association (NBA) while Goswami allegedly replied that he might meet the Prime Minister regarding the matter.

For more information about other articles related to this, visit our website www.thehackerstalk.com

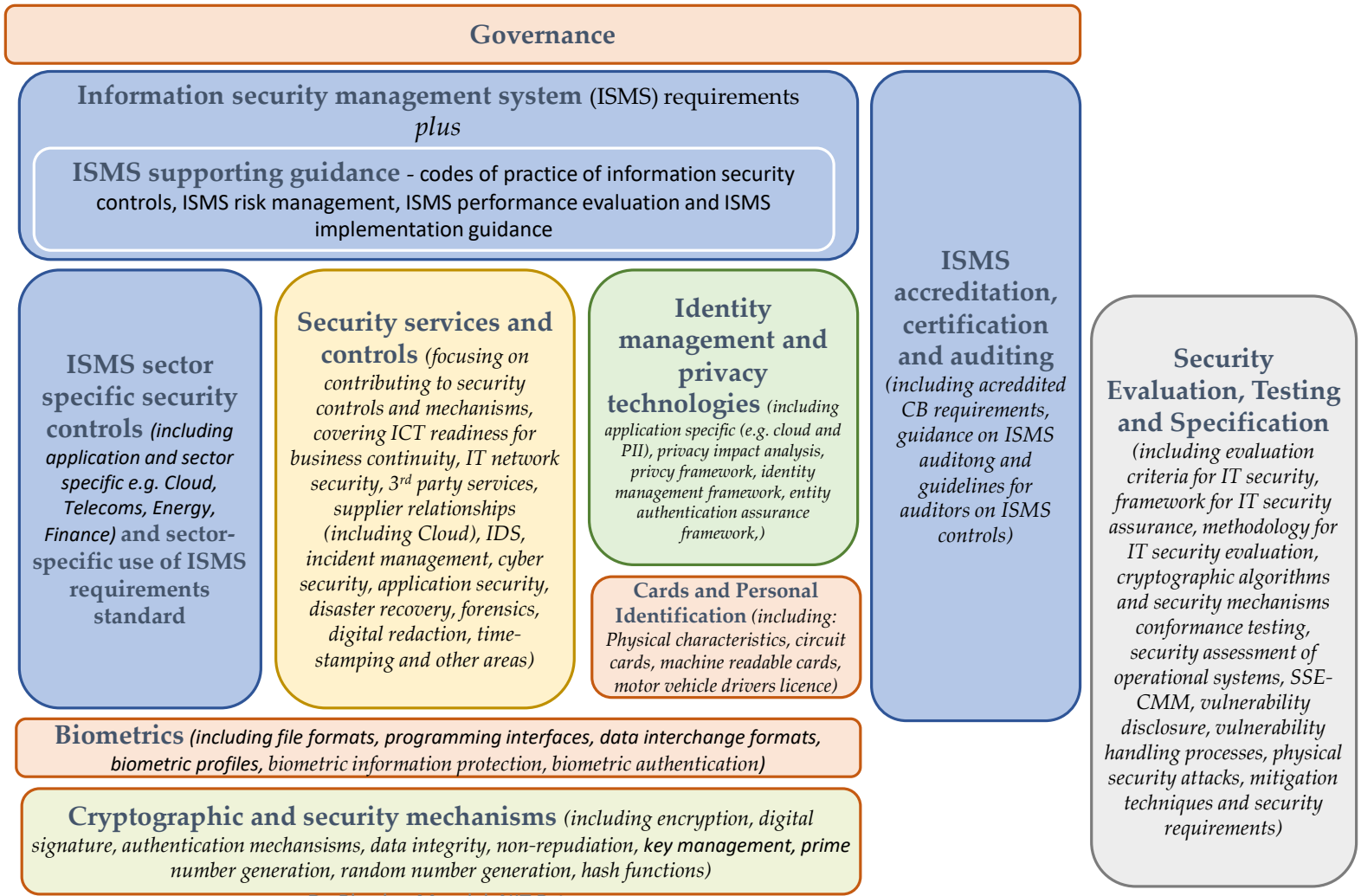
#cybersecurity #ceo #ciso #euinac #security #databreach #privacy #informationsecurity #intelligence #cyberattack #hacking #thehackerstalk #cybernews #darkweb #hacking



Policy to Procedure



Security and Privacy Topic Areas



policy creation on items

- Passwords
- Patch management
- Employee hiring and termination practices
- Backup practices and storage requirements
- Security awareness training
- Antivirus
- System setup and configuration

Security Policy

- top tier of formalized security documents.
- These high-level documents offer a general statement about the organization's assets and what level of protection they should have.
- Well-written policies should spell out who's responsible for security,
- what needs to be protected, and
- what is an acceptable level of risk.
- strategic plan to outline what should be done but don't specifically dictate how to accomplish the stated goals.
- Those decisions are left for standards, baselines, and procedures.
- Security policies can be written to meet advisory, informative, and regulatory needs. Each has a unique role or function.

Advisory Policy

- consequences of certain behavior and actions
- Illegal copying: Employees should never download or install any commercial software, shareware, or freeware onto any network drives or disks unless they have written permission from the network administrator. Be prepared to be held accountable for your actions, including the loss of network privileges, written reprimand, probation, or employment termination if the Rules of Appropriate Use are violated.

Informative Policy

his type of policy isn’t designed with enforcement in mind; it is developed for education. Its goal is to inform and enlighten employees. The following is an example informative policy:

In partnership with Human Resources, the employee ombudsman's job is to serve as an advocate for all employees, providing mediation between employees and management. This job is to help investigate complaints and mediate fair settlements when a third party is requested.

Regulatory Policy

- These policies are used to make certain that the organization complies with local, state, and federal laws. An example regulatory policy might state:

- Because of recent changes to Texas State law, The Company will now retain records of employee inventions and patents for 10 years; all email messages and any backup of such email associated with patents and inventions will be stored for one year.

Standards

Standards are much more specific than policies.

Standards are tactical documents because they lay out specific steps or processes required to meet a certain requirement.

As an example, a standard might set a mandatory requirement that all email communication be encrypted. So, although it does specify a certain standard, it doesn't spell out how it is to be done. That is left for the procedure.

IT Security

Standards/Guidelines

- ISO/IEC 27001 and following
- NIST SP 800-53
- NIST SP 800-82
- ISO/IEC 15408: Common Criteria
- ISA SP99
- IEC 62443
- VDI/VDE 2182
- IEC 62351
- VdS 3473

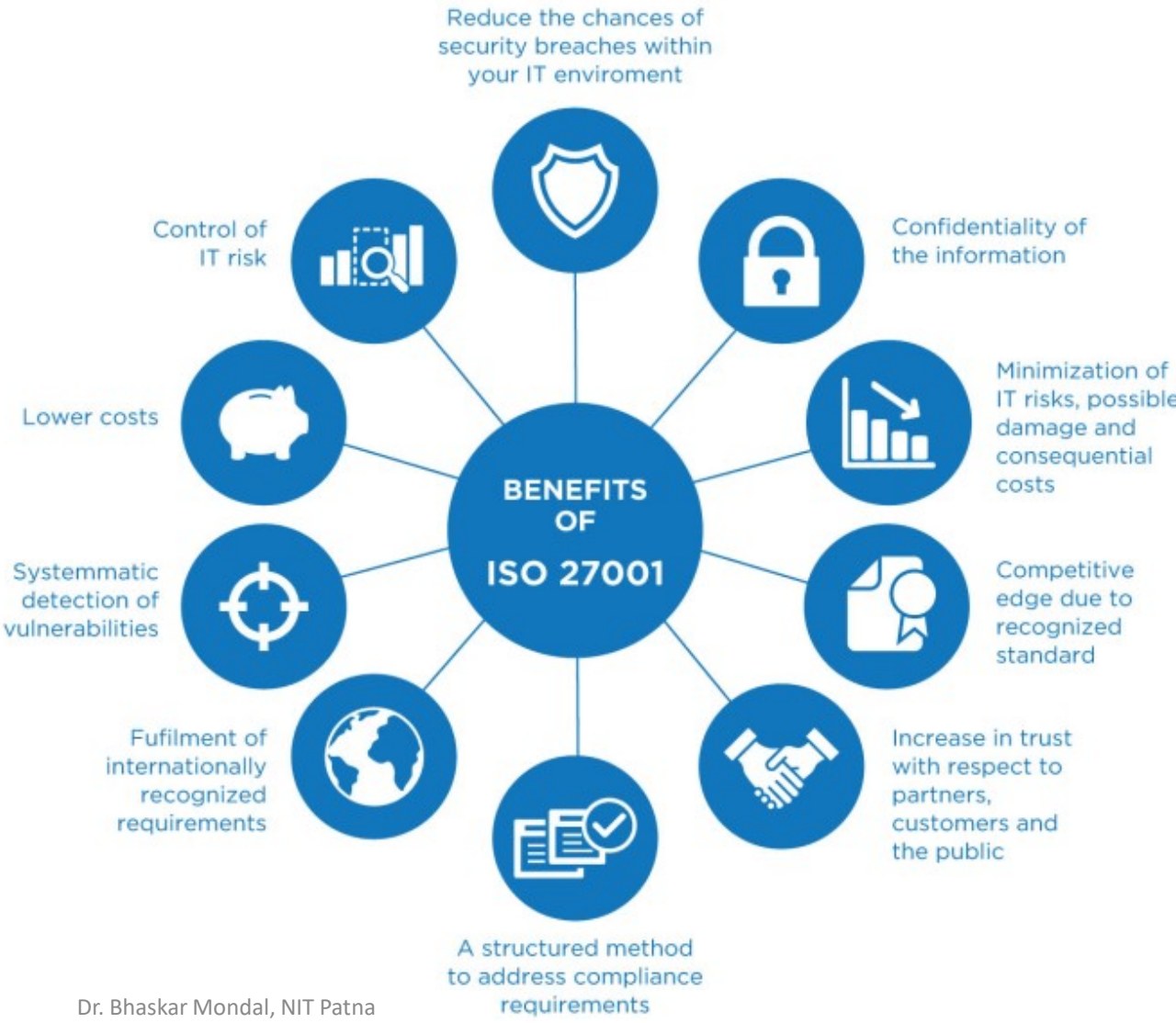
Manufacturer Associations/Authorities

- PROFINET Security Guideline
- Securing EtherNet/IP Networks
- NAMUR NA 115, NE 153
- BSI: *Industrial Control System Security and others*
- SANS – *Critical Controls for Effective Cyber Defense*
- Homeland Security / ICS-CERT

Laws/Regulations

- IT Security Act
- Directive Determining Critical Infrastructures According to the BSI Act (BSI-KritisV)
- Act on Electricity and Gas Supply (Energy Industry Act – EnWG)
- Security catalogue according to § 11 para. 1a EnWG

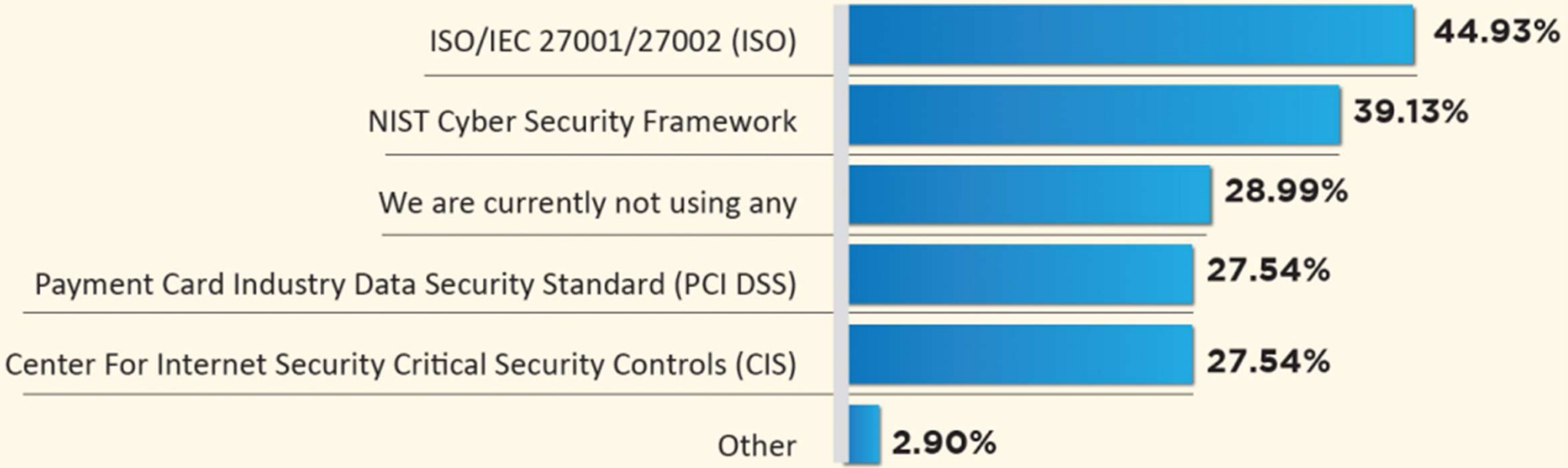
ISO 27001


Reduce the chances of security breaches within your IT enviroment
Control of IT risk
Confidentiality of the information
Lower costs
Minimization of IT risks, possible damage and consequential costs
BENEFITS OF ISO 27001
Systemmatic detection of vulnerabilities
Competitive edge due to recognized standard
Fufilment of internationally recognized requirements
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements

Industry Standard & Frameworks

FIGURE 16:

Leveraging Industry Standards & Frameworks



Health Insurance Portability and Accountability Act (us 1996)

General Data Protection Regulation (EU 2016/679)

GDPR checklist:

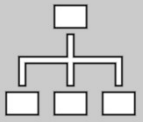
1. Is personal data processed in your company?
2. Is GDPR applicable to your company?
3. Do you process special categories of personal data?
4. What does a national legislation provide?
5. Is the PD transmitted to third countries or international organizations?
6. What role does your company play in data processing?
7. Do all policies and other corporate documents relating to the processing of personal data comply with the Regulation?
8. Data Protection Impact Assessment. When? How? What?
9. Do you need a Data Protection Officer (DPO)?
10. Are processors aware of personal data processing policies and responsibilities?

Indian Govt. Initiatives

- Information Security Act 2000 (amended in 2008 retrofitting new crimes)
  - Legal recognition
  - Electronic docs
  - Digital signature
  - Transaction done using Computer and Internet
  - Describes punishment and Penalty for criminals and contraventions
- Cyber crime cell under CBI
- Cyber crime Police stations (Bangalore got 1st PS in India)
- Data Security Council of India (DSCI)

Baselines

A baseline is a minimum level of security that a system, network, or device must adhere to.



Baselines are usually mapped to industry standards.

As an example, an organization might specify that all computer systems comply with a minimum Trusted Computer System Evaluation Criteria (TCSEC) C2 standard.

Guidelines

- A guideline points to a statement in a policy or procedure by which to determine a course of action.
- It’s a recommendation or suggestion of how things should be done.
- It is meant to be flexible so it can be customized for individual situations.

Procedures

A procedure is the most specific of security documents.

A procedure is a detailed, in-depth, step-by-step document

details exactly what is to be done.

As an analogy, secret recipe for a three-layer cake, it described step by step what needed to be done and how. It even specified a convection oven, which stated was an absolute requirement.

Information Security Approach

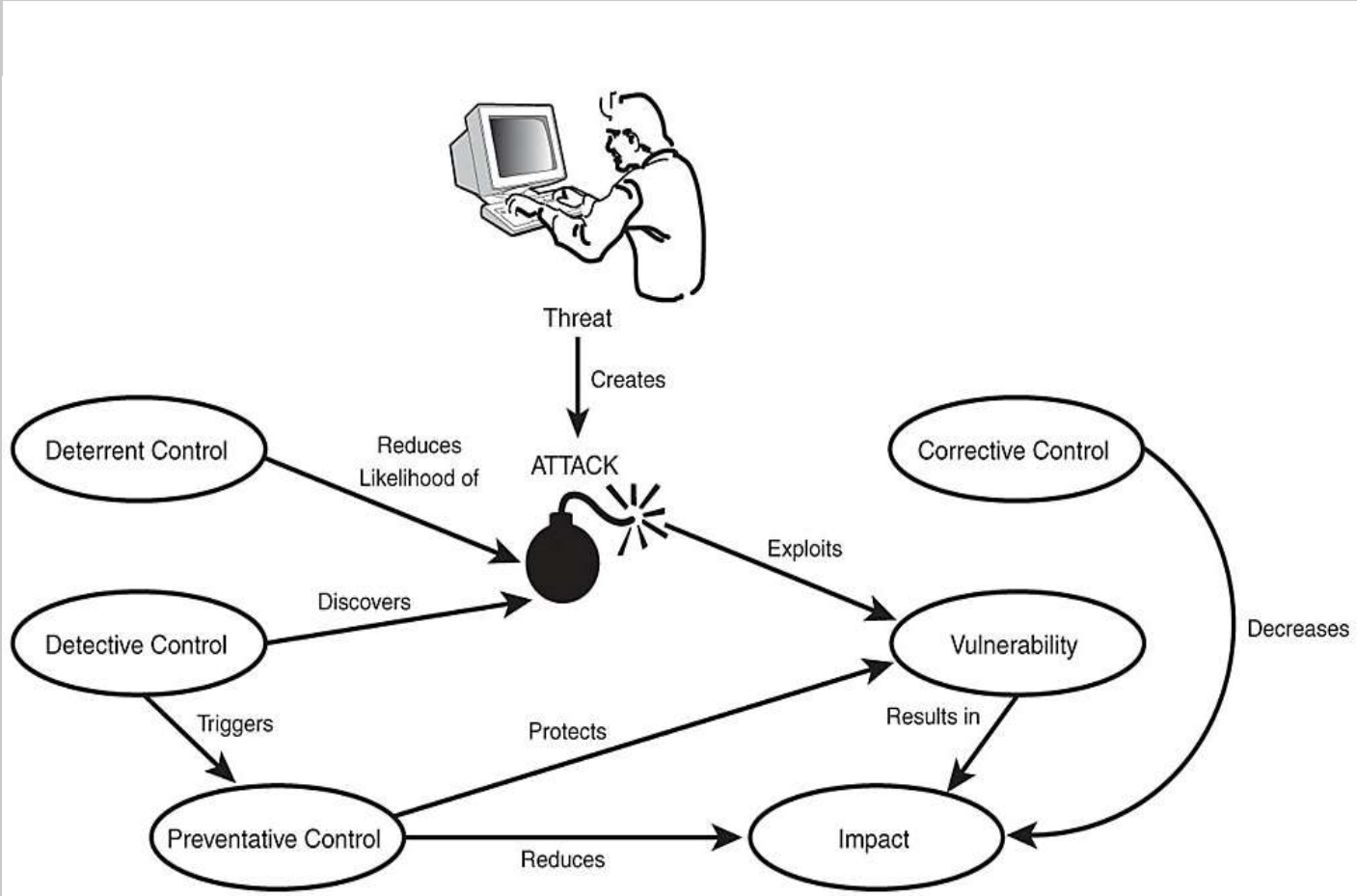
Security Audit tools

- WPscan (vulnerability scanner for Wordpress) http://wpscan.org/
- SQLmap (SQL injection vulnerability scanner) http://sqlmap.org/
- Xenotix (XSS injection vulnerability scanner) http://xenotix.in/
- Metasploit (most advanced security framework) https://www.metasploit.com

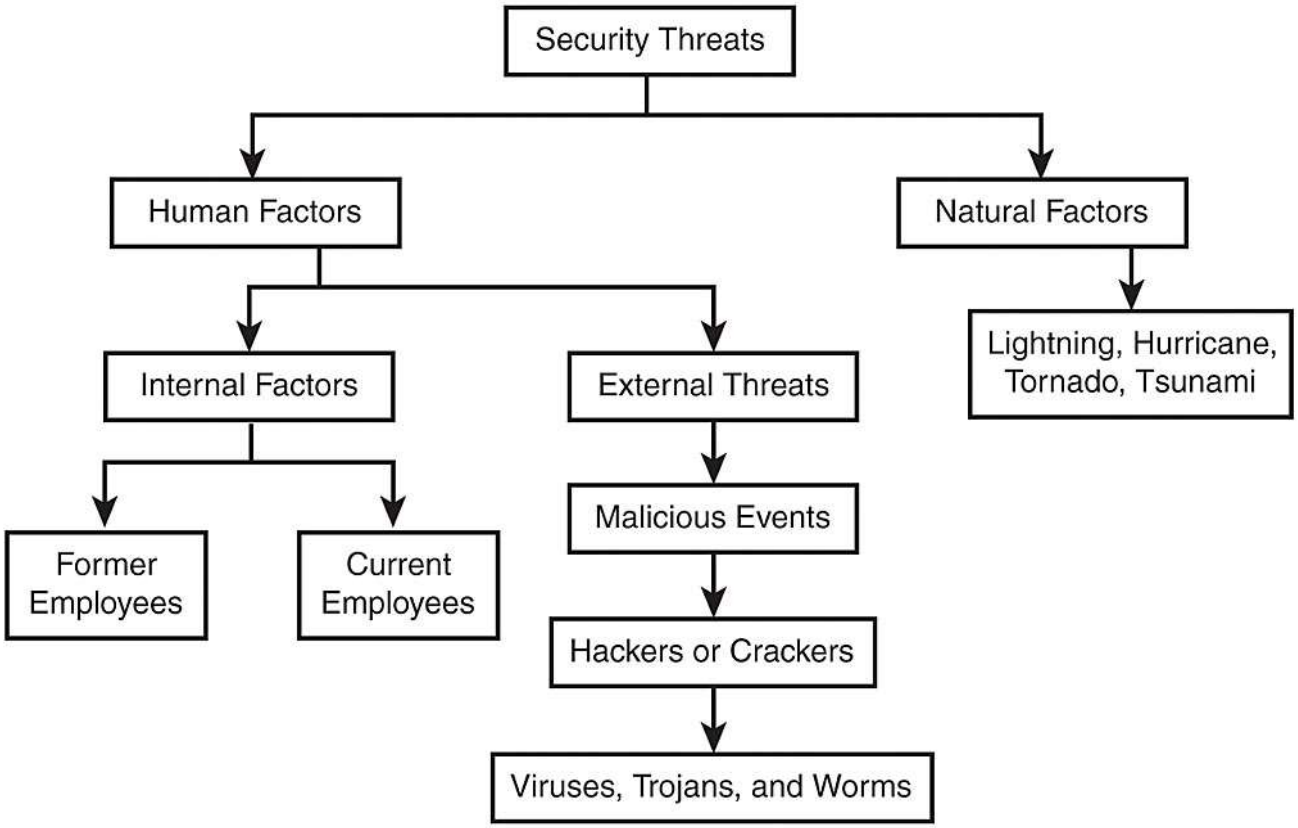
Where security meets ethical limits

- Punkspider (free database of vulnerable websites) https://www.punkspider.org/
- Sarento (Ransomware-as-a-Service) http://encryptor3awk6px.onion/

Threats, vulnerabilities, and controls



https://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4



Security threats

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

Risk-Management Team

- Information system security
- IT and operations management
- System and network administration
- Internal audit
- Physical security
- Business process and information owners
- Human resources
- Legal
- Physical safety

Quantitative Assessment

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

Threat, Vulnerability, and Risk

Threat Type	Threat	Exploit/Vulnerability	Exposed Risk
Human factor internal threat	Intruder	No security guard or controlled entrance	Theft
Human factor external threat	Hacker	Misconfigured firewall	Stolen credit card information
Human factor internal threat	Current employee	Poor accountability; no audit policy	Loss of integrity; altered data
Natural	Fire	Insufficient fire control	Damage or loss of life
Natural	Hurricane	Insufficient preparation	Damage or loss of life
Malicious external threat	Virus	Out-of-date antivirus software	Virus infection and loss of productivity
Technical internal threat	Hard drive failure	No data backup	Data loss and unrecoverable downtime

Qualitative Assessment

Asset	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Customer database	High	High	Medium
Internal documents	Medium	Medium	Low
Advertising literature	Low	Medium	Low
HR records	High	High	Medium

Placing a monetary Value on Assets and elements

- asset value
- Impact
- threat frequency
- safeguard effectiveness
- safeguard costs
- uncertainty, and
- probability

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

Estimate potential losses (SLE)

- This step involves determining the *single loss expectancy (SLE)*.
- SLE is calculated as follows:

$$Single\ loss\ expectancy\ \times\ Asset\ value = Exposure\ factor$$

How SLE, ARO, and ALE

Asset	Risk	Asset Value	Exposure Factor	SLE	Annualized Frequency	ALE
Customer database	Hacked	$432,000	.74	$320,000	.25	$80,000
Word documents and data files	Virus	$9,450	.17	$ 1,650	.9	$1,485
Domain controller	Server failure	$82,500	.88	$ 72,500	.25	$18,125
E-commerce website	DDoS	$250,000	.44	$110,000	.45	$49,500

Conduct a threat analysis (ARO)

estimate the annual rate of occurrence (ARO).

how many times is this expected to happen in one year?

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

Determine annual loss expectancy (ALE)

- This is expressed as annual loss expectancy (ALE).
- ALE is calculated as follows:

$$Annualized\ loss\ expectancy\ (ALE)$$
$$\times\ Single\ loss\ expectancy\ (SLE)$$
$$=\ Annualized\ rate\ of\ occurrence\ (ARO)$$

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

example

- the risk-management team might consult with its experts and determine that 17% of its Word documents and data could be destroyed from a virus.
- The ARO is the frequency at which this event is expected to happen within a given period of time. For example, the experts might have determined that there is a 90% chance of this event occurring within a 1-year period.
- Finally, the ALE is calculated. The ALE is the SLE multiplied by the ARO:
- $1,650 X .9 = $1,485
- This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. You can interpret this figure to mean that the business should expect to lose an average of $1,485 each year due to computer viruses.

Handling Risk

Risk reduction: Implement a countermeasure to alter or reduce the risk.

Risk transference: Purchase insurance to transfer a portion or all of the potential cost of a loss to a third party.

Risk acceptance: Deal with risk by accepting the potential cost and loss if the risk occurs.

Risk rejection: Pretend that the risk doesn't exist and ignore it. Although this is not a prudent course of action, it is one that some organizations choose to take.

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com

Handling Risk

$$Threat \times Vulnerability \times Asset\ value = Total\ risk$$

$$Total\ risk - Countermeasures = Residual\ risk$$

Thank You

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com